



# Safety Instrumented Systems Appreciation Training

A series of presentations for  
managers, operators and maintainers  
of Installed Safety Instrumented Systems.  
Intended to provide awareness  
of the requirements of and compliance to  
IEC 61511.

David Ransome BA, CEng, FInstMC  
Registered Functional Safety Engineer, RFSE  
P & I Design Ltd - Chairman

*P & I Design Ltd*


2 Reed Street

Thornaby

TS17 7AF

01642 617444

<http://www.pidesign.co.uk/>



# Safety Instrumented Systems Appreciation Training - Part 5 Functional Safety Management

David Ransome BA, CEng, FInstMC

Registered Functional Safety Engineer, RFSE

P & I Design Ltd - Chairman

## Purpose!



This presentation is for managers, operators and maintainers. It is intended to provide awareness of the requirements of installed Safety Instrumented Systems complying to IEC 61511.

# Agenda!



To provide an appreciation of:

- Functional Safety Management Systems;
- Functional Safety Assessments,
- FSMS Audits.

Related to IEC 61511 Life-cycle

# Reminder of the SIS Lifecycle



**Operation & Maintenance Phase**  
Typically 10 to 30 times longer than all other phases

**Proof Testing**  
Including Review, Analysis and Failure Monitoring

FSA 4

FSA 4

Operation & Maintenance

De-commissioning

De-commissioning  
Including FSA 5

Modifications  
Including FSA 5's

I  
n  
s  
t  
a  
l  
l  
e  
d  
S  
I  
S

Installation,  
Commissioning & Validation

Handover to end user  
Including FSA 3

**Design**  
Including FSA 2

Design & Engineering

Safety Requirement Specification

**SRS**  
Including FSA 1

HRA & SIF & SIL Determination

**Risk Assessments**

# Functional Safety Management - FSM



Your SIS requires a FSM system, which includes auditable procedures and records, for the following:

- ★ Competency management;
  - HRA and SIL determination;
  - SIS Validation, verification and proof testing ;
  - Operation and Maintenance activities;
  - Management of Change;
- ★ Functional Safety Assessments and audits;
- ★ Monitoring of the SIS performance and corrective actions;
- ★ Configuration Management;
- ★ SIS Security. See HSE delivery guidance on cyber security.

## Competency Management – IEC61511 Clauses 5.2...



Persons, departments or organisations involved in SIS safety lifecycle activities shall be competent to carry out the activities for which they are accountable;

A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing.

# Configuration Management



Although configuration management is more specific to manufactures of components and software development of the SIS, there is a requirement for end users to control changes, with respect to maintaining continuity of the system by ensuring traceability of any changes throughout the SIS lifecycle.

Example:

Update of the safety plc code – version numbers – traceability and audibility of changes

Sensor change – like for like? – Firmware version – Serial Number



## Security Risk Assessment – IEC61511 Clause 8.2.4



This is a new requirement of IEC61511 Ed 2.

End Users shall develop and conduct a risk assessment;

An example for achieving this could be :

- Identify all threats;
- Assign a risk level to each threat;
- Assess the consequence of each threat;
- Identify where vulnerabilities lie;
- Review adequacy of current protection measures;
- Plan and implement additional protection measures.

See additional guidance: ISA TR84.00.09, IEC 27001:2013, IEC 62443-2-1:2010 and HSE delivery guidance on cyber security.

## FSM - Safety Planning – IEC61511 Clause 5.2.4



Safety planning shall take place to define the lifecycle activities, persons, departments, organisations involved, together with their responsibilities;

This plan shall be updated throughout the entire SIS lifecycle.

The safety planning can be incorporated in:

- a section in the quality plan entitled “SIS Safety Lifecycle Plan”; or
- a separate document entitled “SIS Safety Lifecycle Plan”; or
- several documents which may include company procedures or working practices.

## FSM – SIS Performance -IEC61511 Clause 5.2.5.3



Procedures shall be implemented to evaluate the performance of the SIS against its safety requirements to:

- identify and prevent systematic failures;
- assess whether reliability parameters of the SIS are in accordance with those assumed during the design;
- define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design;
- compare the demand rate on the SIF during actual operation with the assumptions made during risk assessment when the SIL requirements were determined.

# Functional Safety Assessments v Audits



## Functional Safety Assessments On the SIS

## Functional Safety Audits On the FSMS

FSA Stage:

- 1 - After HRA & Safety Requirement Specification
- 2 - After Design
- 3 - After pre-commissioning before going into service
- 4 - **Periodically, after gaining operational experience**
- 5 - **Before every modification or de-commissioning**



# Functional Safety Assessments



Functional Safety Assessments are reviews and investigations to check that functional safety has been achieved and remains effective throughout the life of the SIS.

IEC 61511 defines five stages when FSA's shall be conducted, Stages 1, 2 & 3 are during the realisation phases of the SIS.

Stages 4 & 5 are applicable to installed SIS.

# Functional Safety Assessments



For Installed Safety Instrumented Systems, Stage 4 and 5 assessments shall be conducted.

Stage 4 Assessments shall be conducted periodically during the operational phase of the SIS. Typical time scales are 3 – 5 years.

Stage 5 Assessments shall be conducted when a modification is required to the SIS, this also includes the de-commissioning of the SIS.

# Functional Safety Assessments - Team



The FSA shall be carried out by a multi-disciplined team, relevant to the appropriate FSA, representing the necessary disciplines involved in the design, operation, maintenance and management of the SIS. With at least one senior competent person not involved in the operation and maintenance of the SIS (for stages 4 and 5).



## Functional Safety Assessment – Stage 4



Typical team members for a FSA 4:

Chair – A competent assessor of Functional Safety and knowledgeable with IEC61511 but independent to the operation and maintenance of the SIS;

“Functional Safety Manager” – The person responsible for the management of the SIS (possibly the Terminal Manager);

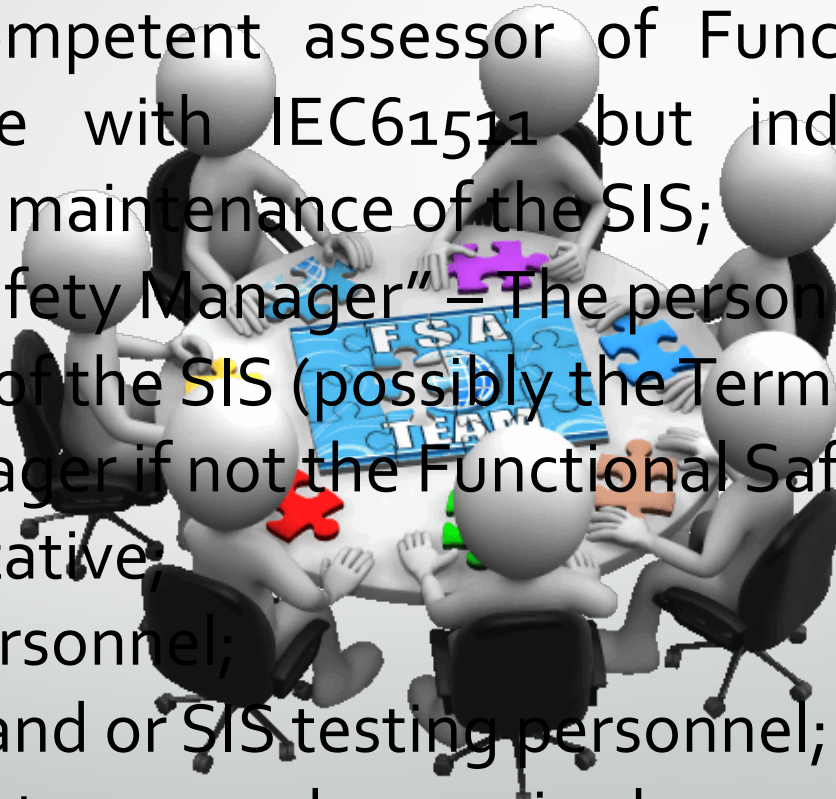
Terminal Manager if not the Functional Safety Manager;

SHE representative;

Operations personnel;

Maintenance and or SIS testing personnel;

Other specialists as may be required.





## Functional Safety Assessment – Stage 4



The FSA 4 should assess how the SIS is performing in relationship to the assumptions made during the design phase.

- Are the assumptions still valid, is the HRA up to date?
- SIS performance, including demands, activations, maintenance, validation and verification activities;
- Review of testing procedures and their effectiveness;
- Management of change procedures are in place and properly implemented.

## Functional Safety Assessment – Stage 4



In addition the following should be reviewed:

- Previous modifications have been implemented;
- Actions from previous FSA's have been resolved;
- The SIS remains designed, constructed and installed in accordance with the SRS;
- Operating, maintenance and emergency procedures;
- Competency management;
- Plans for implementing further FSA's are in place;
- Security risk assessment for the SIS has been produced and reviewed.

## Functional Safety Assessment – Stage 4



If the SIS was not designed and installed to the latest version of IEC61511 then a gap assessment to identify any differences and an implementation plan for improvements, (unless the improvements are shown not to be reasonably practical).

A typical time period for this implementation would be three years from the publication of the revised standard.

# Modification



What is a modification?

A modification, is any change to the SIS other than a like for like replacement of a component.



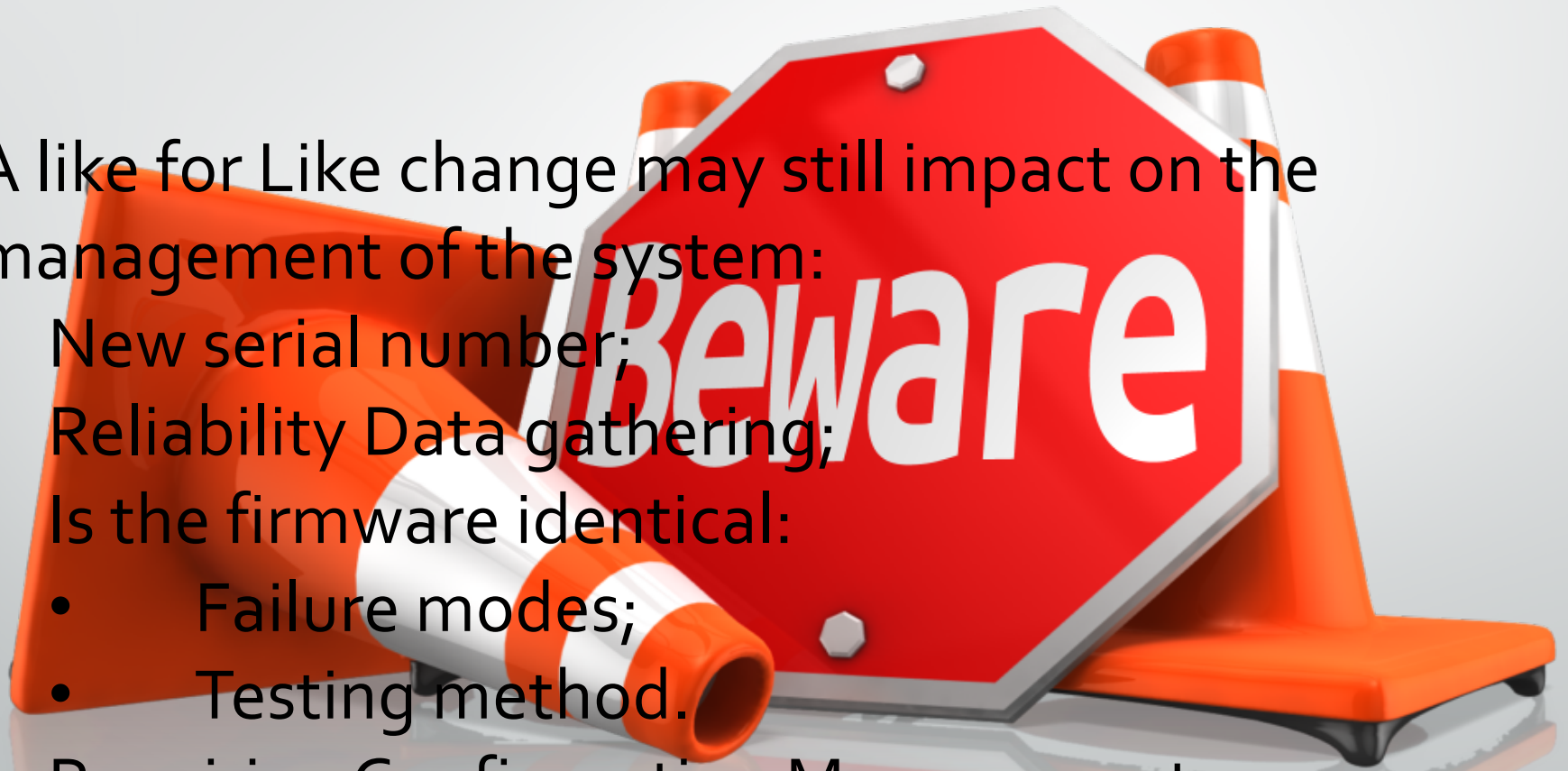
# Modification



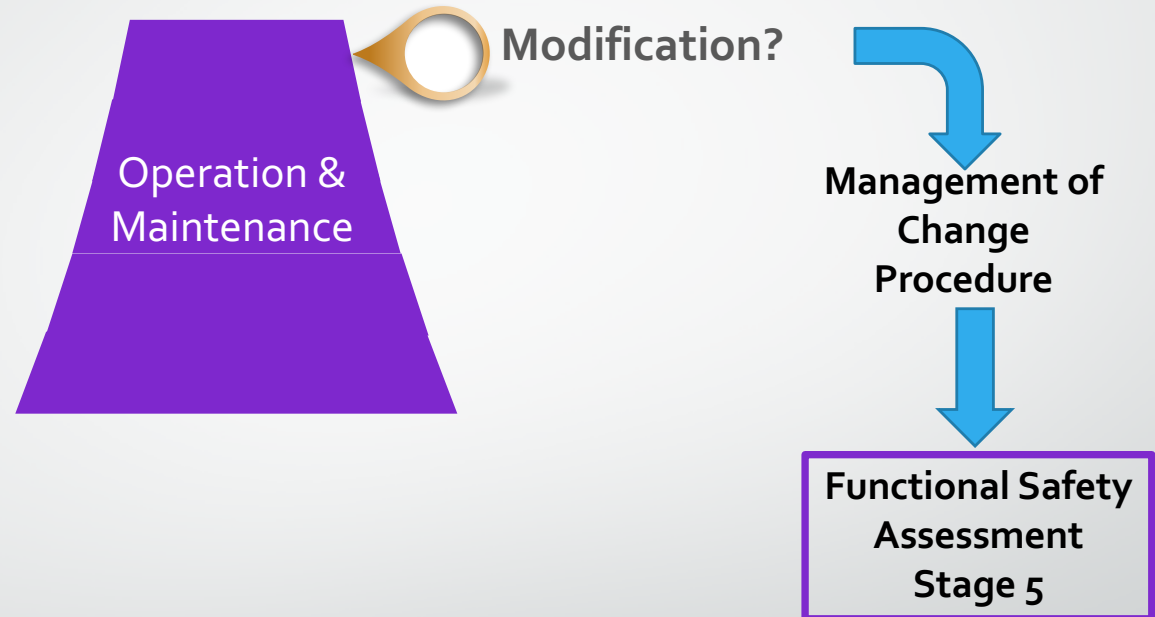
A like for Like change may still impact on the management of the system:

- New serial number;
- Reliability Data gathering;
- Is the firmware identical:
  - Failure modes;
  - Testing method.

Requiring Configuration Management



# SIS Lifecycle - Modification

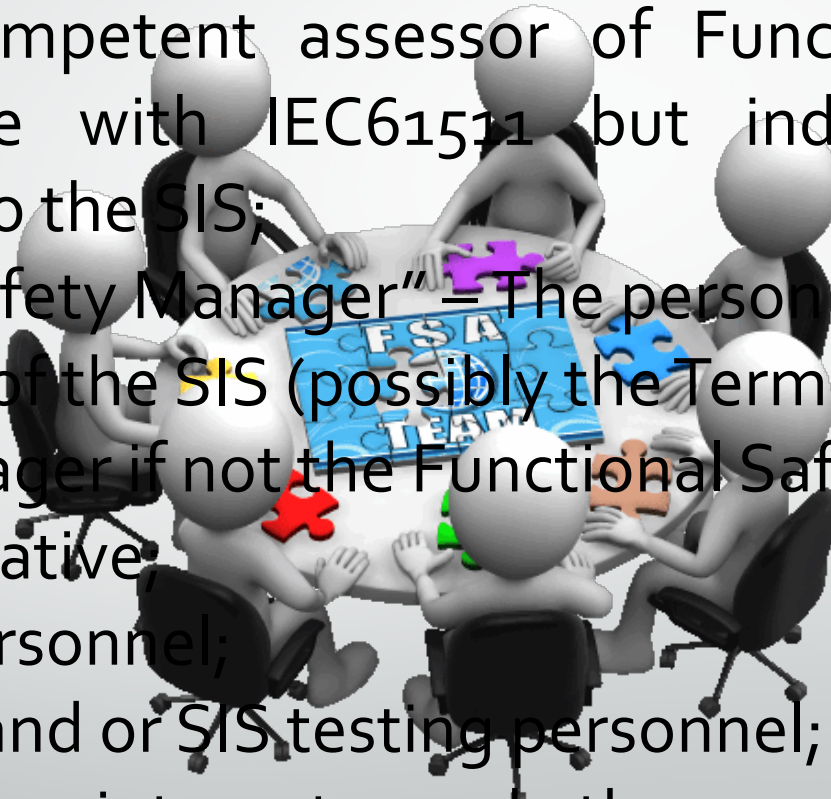


## Functional Safety Assessment – Stage 5



Typical team members for a FSA 5 – End User and specialists:

- Chair – A competent assessor of Functional Safety and knowledgeable with IEC61511 but independent of the modification to the SIS;
- “Functional Safety Manager” – The person responsible for the management of the SIS (possibly the Terminal Manager);
- Terminal Manager if not the Functional Safety Manager;
- SHE representative;
- Operations personnel;
- Maintenance and or SIS testing personnel;
- Designer, system integrator and other required specialists.



## Functional Safety Assessment – Stage 5



The FSA 5 is to verify that when a modification has been performed, it has not compromised the SIS and that the modification performs as intended and all lifecycle documentation reflects the changes.

IEC 61511 Edition 2 states that the modification shall not commence until after the FSA has been completed.

I believe the intent of the clause is that the FSA should have commenced before the modification is performed.



## Functional Safety Assessment – Stage 5



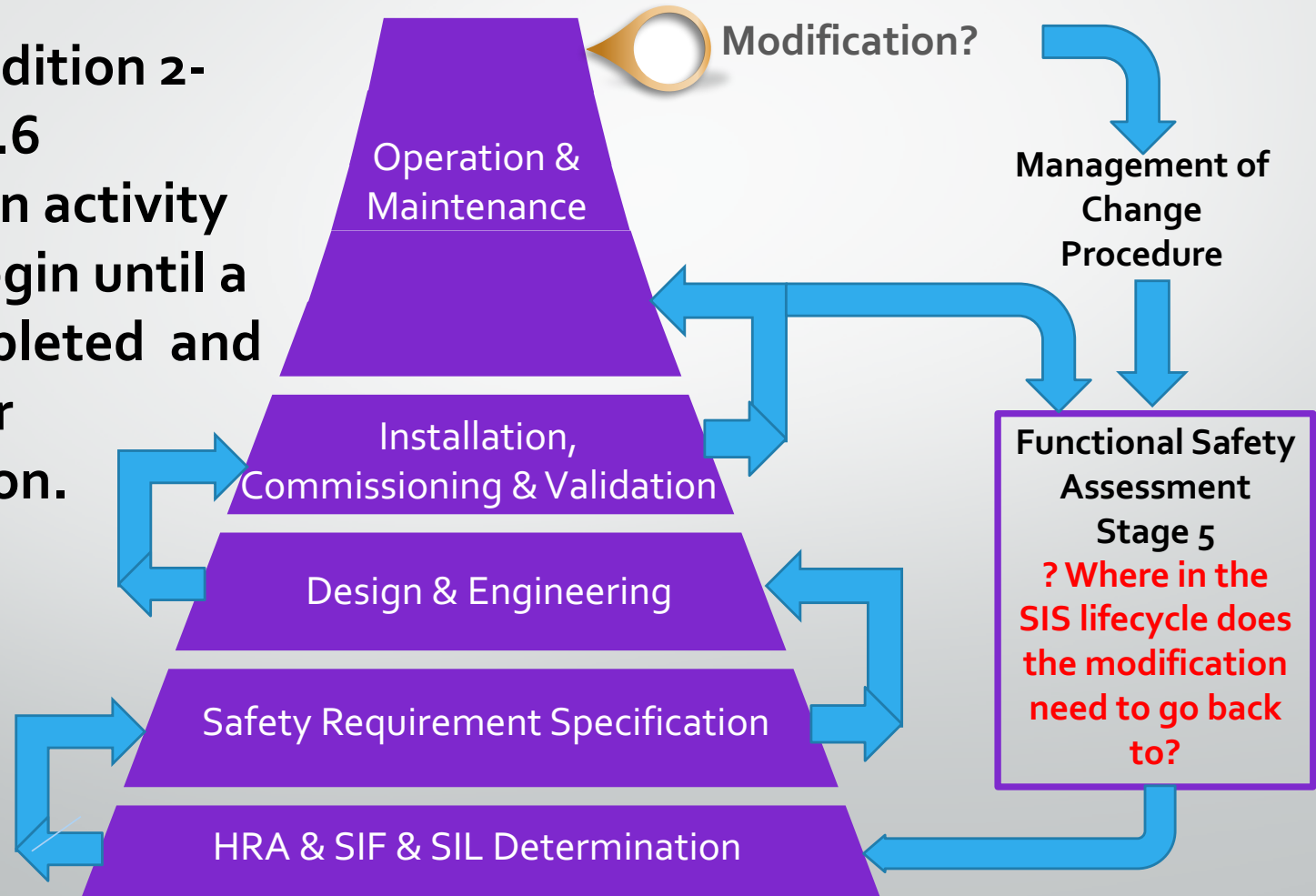
In my experience, it is necessary to fragment the FSA 5.

1. An initial FSA meeting to determine what the modification is, define roles and responsibilities of those involved, assess the impact it has on functional safety and where in the safety lifecycle the modification needs to return to.
2. Following the design of the modification, a detailed review of the lifecycle documentation can be performed.
3. On completion, to ensure functional safety of the modification a review of the installed SIS and as-built lifecycle documentation can be reviewed.

# SIS Lifecycle - Modification



IEC 61511 Edition 2-  
Clause 17.2.6  
Modification activity  
shall not begin until a  
FSA is completed and  
after proper  
authorisation.



## Functional Safety Audits - Overview



The purpose of the Functional Safety Audit is to review SIS procedures and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed.

Including:

- A review of all the SIS policies and procedures;
- An audit that personnel are following the procedures ;
- That the latest version of the procedures are used.

Audits are typically carried out by an independent person familiar with carrying out audits, such as a quality manager, with obvious reference to IEC61511 . Where gaps are identified, improvements should be made.

# Functional Safety Audits – IEC 61511 Clauses



## 5.2.6.2.1

The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.

# Functional Safety Audits – IEC 61511 Clauses



## 5.2.6.2.2

All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.

## Functional Safety Audits – IEC 61511 Clauses



### 5.2.6.2.3

Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited. Procedures shall be defined and executed for auditing compliance with requirements including:

- the frequency of the functional safety audit activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the functional safety auditing activities;
- the recording and follow-up activities.

## Functional Safety Audits – IEC 61511 Clauses



### 5.2.6.2.4

Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).

# Functional Safety Audits – IEC 61511 Clauses



## 5.2.6.2.5

Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).



# Functional Safety Audits



Remember –

If it is not documented or recorded.

It doesn't exist!

## IEC 61511 Ed 2 – Salient Points



- The word should has been replaced with SHALL in many clauses;
- Management of Change procedures for SIS mandatory;
- All functional safety assessments and audits mandatory;
- Plans and procedures to improve functional safety management shall be developed and maintained;
- Requires end users to collect and analyse reliability data;
- Requirement to review and risk assess SIS security.

The End!





*P & I  
DESIGN*



2 Reed Street,  
Gladstone Industrial Estate,  
Thornaby TS17 7AF  
**Tel:** +44 (0) 1642 617444  
**Fax:** +44 (0) 1642 616447  
**Email:** [sales@pidesign.co.uk](mailto:sales@pidesign.co.uk)  
[www.pidesign.co.uk](http://www.pidesign.co.uk)



Produced by [www.billinghampress.co.uk](http://www.billinghampress.co.uk)

P & I Design Limited